Security Guidelines for Personnel Who Work from a Telecommuting Center

The U.S. House of Representatives (House) is committed to providing secure means of working from alternative work sites, such as telecommuting centers. A higher level of responsibility for information security lies with remote users because the employee works unobserved and the work environment falls outside the physical protection of a House facility.

Remote users must take and accept a higher level of responsibility for all Congressional electronic information and data accessed by them from outside the physical protection of the House network.

Employees who work at telecommuting centers need to be aware of the risk of inadvertent disclosure of House information. Reasonable precautions must be taken to protect House information from loss, theft, damage, and misuse. These precautions must apply no matter where the information is located and no matter what form it takes. House employees are responsible for ensuring that no House information, whether printed or electronic, remains at the telecommuting location when the employee's work is completed.

Remote users must:

1. Protect the information entrusted to them.

2. Fill in the attached information sheet while in the central office and print the proper configuration instructions from: http://onlinecao.house.gov/download/dialaccess2.htm

3. Use special security measures such as changing passwords often and using an authentication device, e.g. SecurID, for a secure connection. Approved remote access authentication devices are provided by the House Information Resources (HIR) Information Systems Security Office.

4. Follow the instructions (you printed in step #2) for creating and using profiles with Microsoft Exchange.

5. Be alert for anomalies and vulnerabilities and report security incidents to the telecommuting center and

House Information Resources at (202) 225-6002.

6. Use a password-protected screen saver that activates after a predetermined period of inactivity; the recommended interval is ten minutes.

7. Access only those House systems necessary to perform their jobs.

8. Use House network shared drives to save information, rather than local hard disk drives or diskettes.

9. Delete all temporary and cache files stored on the local hard disk drive.

10. Remove all Exchange/Outlook profile information that was created on the computer for the purpose of your connecting to the House.

11. Remove the Dial-up Networking configuration used to connect to the House.

12. Remove any password files created on the system for you. These files would have a .pwl extension and begin with your login name. Example usernam.pwl. A search of the hard drive will reveal the location of these files.

13. Empty the recycle bin as the last step prior to shutting down the system.

14. Contact the HIR
Call Center,
(202) 225-6002, with questions about configuring dial and email services or for help in deleting information copied to non-House computers.

Users must ensure the Telecommuting
Center:

1. Provides a physical environment where House users are able to protect their information from unauthorized observers.

2. Provides computers with modems and dial-in access to the House backbone using a House-approved authentication device.

3. Have Has current anti-virus software installed and operational.

4. Ensure Guarantees that computers in use by House personnel are not connected to the telecommuting center's local network.

REMOTE DIAL SETUP INFORMATION SHEET

Please see your systems administrator for the following information, which is necessary for remote access to an NT server or House Exchange email servers.

User/Email Information:

Windows NT Server Name: _____

Windows NT Domain Name: _____

Personal Drive Mappings on NT Server: _____

NT Username: _____

Exchange Alias: _____

Exchange Server name: _____